Terms used **exponent** and **crypto key** Found **3,307** of **198,146**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Crypto backup and key escrow
David Paul Maher
March 1996 **Communications of the ACM**, Volume 39 Issue 3
Publisher: ACM Press
Full text available: pdf(498.27 KB) Additional Information: full citation, references, citings, index terms

2 Applied cryptography II: Deniable authentication and key exchange
Mario Di Raimondo, Rosario Gennaro, Hugo Krawczyk
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(266.22 KB) Additional Information: full citation, abstract, references, index terms

We extend the definitional work of Dwork,Naor and Sahai from deniable authentication to deniable key-exchange protocols. We then use these definitions to prove the deniability features of SKEME and SIGMA, two natural and efficient protocols which serve as basis for the Internet Key Exchange (IKE)protocol.SKEME is an encryption-based protocol for which we prove full deniability based on the plaintext awareness of the underlying encryption scheme. Interestingly SKEME's deniability is possibly the ...

Keywords: authentication, deniability, key exchange

3 Computer security: Implementation of fast RSA key generation on smart cards
Chenghuai Lu, Andre L. M. dos Santos, Francisco R. Pimentel
March 2002 **Proceedings of the 2002 ACM symposium on Applied computing SAC '02**
Publisher: ACM Press
Full text available: pdf(645.79 KB) Additional Information: full citation, abstract, references, citings, index terms

Although smart cards are becoming used in an increasing number of applications, there is small literature of the implementation issues for smart cards. This paper describes the issues and considerations that need to be taken into account when implementing the key generation step of a cryptographic algorithm widely used nowadays, RSA.Smart cards are used in many applications that require a tamper resistant area. Therefore, smart cards that use cryptography have to provide encryption, decryption, ...

Keywords: RSA key generation, coprocessor, prime finding, smart card

4 Verifiable partial key escrow
Mihir Bellare, Shafi Goldwasser
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security CCS '97**
Publisher: ACM Press
Full text available: Additional Information:

pdf(1.98 MB) full citation, references, citings, index terms

5 Digital circuits design: Current mask generation: a transistor level security against DPA attacks

Daniel Mesquita, Jean-Denis Techer, Lionel Torres, Gilles Sassatelli, Gaston Cambon, Michel Robert, Fernando Moraes

September 2005 **Proceedings of the 18th annual symposium on Integrated circuits and system design SBCCI '05**

Publisher: ACM Press

Full text available: pdf(513.86 KB) Additional Information: full citation, abstract, references, index terms

The physical implementation of cryptographic algorithms may leak to some attacker security information by the side channel data, as power consumption, timing, temperature or electromagnetic emanation. The Differential Power Analysis (DPA) is a powerful side channel attack, based only on the power consumption information. There are some countermeasures proposed at algorithmic or architectural level that are expensive and/or complexes. This paper addresses the DPA attack problem by a novel and eff ...

Keywords: DPA, countermeasures, cryptography, side channel attacks

6 Cryptosystems: Paillier's cryptosystem revisited

Dario Catalano, Rosario Gennaro, Nick Howgrave-Graham, Phong Q. Nguyen

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**

Publisher: ACM Press

Full text available: pdf(1.55 MB) Additional Information: full citation, abstract, references, citings, index terms

We re-examine Paillier's cryptosystem, and show that by choosing a particular discrete log base g, and by introducing an alternative decryption procedure, we can extend the scheme to allow an arbitrary exponent e instead of N. The use of low exponents substantially increases the efficiency of the scheme. The semantic security is now based on a new *decisional* assumption, namely the hardness of deciding whether an element is a "small" e-th residue modulo N ...

7 Efficient generation of shared RSA keys

Dan Boneh, Matthew Franklin

July 2001 **Journal of the ACM (JACM)**, Volume 48 Issue 4

Publisher: ACM Press

Full text available: pdf(202.94 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe efficient techniques for a number of parties to jointly generate an RSA key. At the end of the protocol an RSA modulus $N = pq$ is publicly known. None of the parties know the factorization of N. In addition a public encryption exponent is publicly known and each party holds a share of the private exponent that enables threshold decryption. Our protocols are efficient in computation and communication. All results are presented in the *honest but curious* scena ...

Keywords: Multiparty computation, RSA, primality testing, threshold cryptography

8 Some facets of complexity theory and cryptography: A five-lecture tutorial

Jörg Rothe

December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(2.78 MB) Additional Information: full citation, abstract, references, citings, index terms, review

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key

cryptography, zero-knowledge protocols

9 On the importance of securing your bins: the garbage-man-in-the-middle attack
Marc Joye, Jean-Jacques Quisquater
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security CCS '97**
Publisher: ACM Press
Full text available: pdf(812.52 KB) Additional Information: full citation, references, index terms

10 URSA: ubiquitous and robust access control for mobile ad hoc networks
Haiyun Luo, Jiejun Kong, Petros Zerfos, Songwu Lu, Lixia Zhang
December 2004 **IEEE/ACM Transactions on Networking (TON)**, Volume 12 Issue 6
Publisher: IEEE Press
Full text available: pdf(836.70 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Restricting network access of routing and packet forwarding to well-behaving nodes and denying access from misbehaving nodes are critical for the proper functioning of a mobile ad-hoc network where cooperation among all networking nodes is usually assumed. However, the lack of a network infrastructure, the dynamics of the network topology and node membership, and the potential attacks from inside the network by malicious and/or noncooperative selfish nodes make the conventional network access co ...

Keywords: mobile ad hoc networks, self-organized access control

11 Relating cryptography and formal methods: a panel
Michael Backes, Catherine Meadows, John C. Mitchell
October 2003 **Proceedings of the 2003 ACM workshop on Formal methods in security engineering FMSE '03**
Publisher: ACM Press
Full text available: pdf(710.65 KB) Additional Information: full citation, abstract, references, index terms

Bridging the gap between formal methods and cryptography has recently received a lot of interest, i.e., investigating to what extent proofs of cryptographic protocols made with abstracted cryptographic operations are valid for real implementations. This led to the notion of cryptographically faithful (sound) abstractions. These abstractions allow for a provably secure cryptographic implementation; however their incorporation into machine-aided verification of security protocols has not been p ...

Keywords: cryptography, formal methods, security protocols

12 Security protocols: Improving secure server performance by re-balancing SSL/TLS handshakes
Claude Castelluccia, Einar Mykletun, Gene Tsudik
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(327.25 KB) Additional Information: full citation, abstract, references

Much of today's distributed computing takes place in a client /server model. Despite advances in fault tolerance - in particular, replication and load distribution -- server overload remains to be a major problem. In the Web context, one of the main overload factors is the direct consequence of expensive Public Key operations performed by servers as part of each SSL handshake. Since most SSL-enabled servers use RSA, the burden of performing many costly decryption operations can be very detriment ...

Keywords: client puzzles, denial-of-service, hardware accelerators, load-balancing, server-aided RSA, server-aided secure computation

13 Quasi-Random Number Sequences from a Long-Period TLP Generator with Remarks on Application to Cryptography
Herbert S. Bright, Richard L. Enison

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(1.18 MB) Additional Information: full citation, references, citings, index terms

14 Timing attacks on RSA: revealing your secrets through the fourth dimension
Wing H. Wong
May 2005 **Crossroads**, Volume 11 Issue 3
Publisher: ACM Press
Full text available: html(31.40 KB) Additional Information: full citation, references, index terms

15 Finding smooth integers in short intervals using CRT decoding
Dan Boneh
May 2000 **Proceedings of the thirty-second annual ACM symposium on Theory of computing STOC '00**
Publisher: ACM Press
Full text available: pdf(712.12 KB) Additional Information: full citation, references, citings, index terms

16 A k-th order Carmichael key scheme for shared encryption
Selwyn Russell
April 1997 **ACM SIGSAC Review**, Volume 15 Issue 2
Publisher: ACM Press
Full text available: pdf(118.65 KB) Additional Information: full citation, abstract, references, index terms

A generalization of a digital multisignature key scheme published by Desmedt and Frankel is presented, with increased protection from line monitors and with a high degree of privacy of message contents.

The Desmedt/Frankel paper at Crypto'91 [1] presented the following shared encryption Carmichael scheme:

• An RSA cryptosystem with modulus n and private key K Priv.

• Separate individual keys K Priv_i are generated by ...

17 Cryptosystems: Securely combining public-key cryptosystems
Stuart Haber, Benny Pinkas
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**
Publisher: ACM Press
Full text available: pdf(416.51 KB) Additional Information: full citation, abstract, references, citings, index terms

It is a maxim of sound computer-security practice that a cryptographic key should have only a single use. For example, an RSA key pair should be used only for public-key encryption or only for digital signatures, and not for both.In this paper we show that in many cases, the simultaneous use of related keys for two cryptosystems, e.g. for a public-key encryption system and for a public-key signature system, does not compromise their security. We demonstrate this for a variety of public-key encry ...

18 Enhancing privacy and trust in electronic communities
Bernardo A. Huberman, Matt Franklin, Tad Hogg
November 1999 **Proceedings of the 1st ACM conference on Electronic commerce EC '99**
Publisher: ACM Press
Full text available: pdf(172.79 KB) Additional Information: full citation, references, citings, index terms

19 An unknown key-share attack on the MQV key agreement protocol
Burton S. Kaliski
August 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4

Issue 3
Publisher: ACM Press
Full text available: pdf(119.07 KB) Additional Information: full citation, abstract, references, citings, index terms

The MQV key agreement protocol, a technique included in recent standards, is shown in its basic form to be vulnerable to an unknown key-share attack. Although the attack's practical impact on security is minimal---a key confirmation step easily prevents it---the attack is noteworthy in the principles it illustrates about protocol design. First, minor "e;efficiency improvements"e; can significantly alter the security properties of a protocol. Second, protocol analysis must consider potent ...

Keywords: Key agreement, MQV, protocol design, unknown key-share attack

20 Signature schemes based on the strong RSA assumption

Ronald Cramer, Victor Shoup
August 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(168.52 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe and analyze a new digital signature scheme. The new scheme is quite efficient, does not require the signer to maintain any state, and can be proven secure against adaptive chosen message attack under a reasonable intractability assumption, the so-called strong RSA assumption. Moreover, a hash function can be incorporated into the scheme in such a way that it is also secure in the random oracle model under the standard RSA assumption.

Keywords: RSA, digital signatures, provable security

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next